Jan 19, 2023 by **maia arson crimew** in **security**, **infosec**, **jenkins**, **aviation**, **nofly**

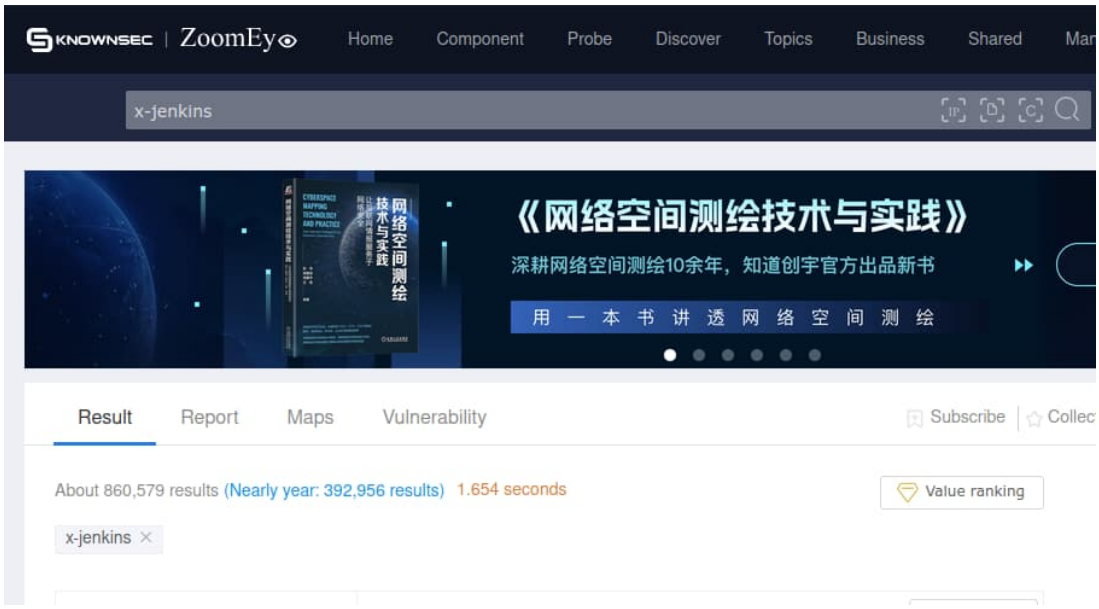
how to completely own an airline in 3 easy steps

and grab the TSA nofly list along the way

> note: this is a slightly more technical* and comedic write up of the story covered by my friends over at dailydot, which you can read here
>
> *i say slightly since there isnt a whole lot of complicated technical stuff going on here in the first place

step 1: boredom

like so many other of my hacks this story starts with me being bored and browsing shodan (or well, technically zoomeye, chinese shodan), looking for exposed jenkins servers that may contain some interesting goods. at this point i've probably clicked through about 20 boring exposed servers with very little of any interest, when i suddenly start seeing some familar words. "ACARS", lots of mentions of "crew" and so on. lots of words i've heard before, most likely while binge watching Mentour Pilot YouTube videos. jackpot. an exposed jenkins server belonging to CommuteAir.



step 2: how much access do we have really?

ok but let's not get too excited too quickly. just because we have found a funky jenkins server doesn't mean we'll have access to much more than build logs. it quickly turns out that while we don't have anonymous admin access (yes that's quite frequently the case [god i love jenkins]), we do have access to build workspaces. this means we get to see the repositories that were built for each one of the ~70 build jobs.

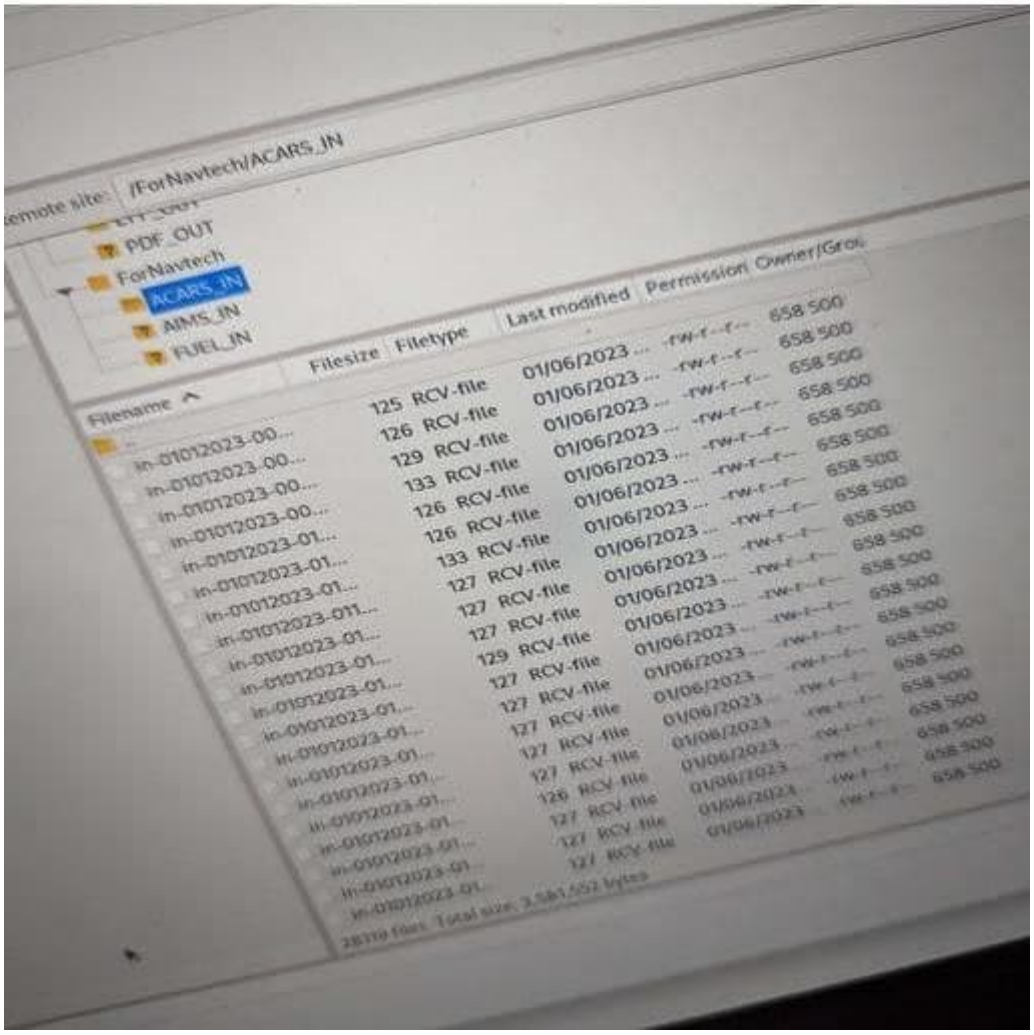
step 3: let's dig in

most of the projects here seem to be fairly small spring boot projects. the standardized project layout and extensive use of the resources directory for configuration files will be very useful in this whole endeavour.

the very first project i decide to look at in more detail is something about "ACARS incoming", since ive heard the term acars before, and it sounds spicy. a quick look at the resource directory reveals a file called `application-prod.properties` (same also for `-dev` and `-uat`). it couldn't just be that easy now, could it?

well, it sure is! two minutes after finding said file im staring at filezilla connected to a navtech sftp server filled with incoming and outgoing ACARS messages. this aviation shit really do get serious.

this aviation shit get serious



here is a sample of a departure ACARS message:

```
~/bounty/commutair  20:41:44
$ cat in-01012023-003509-1136486_DEP.RCV
```

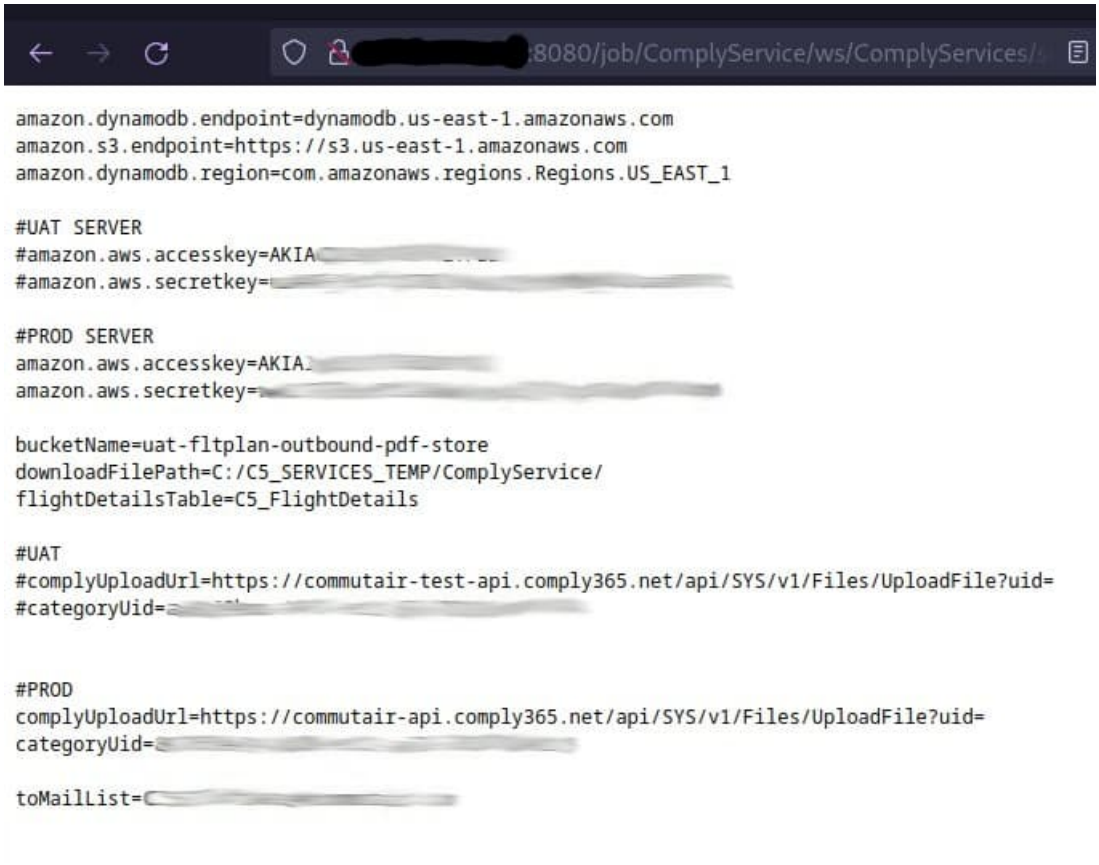
File: **in-01012023-003509-1136486_DEP.RCV**

```
1
2   ^AQU CLEADC5
3   .DDLXCXA 010035
4   ^BDEP
5   FI C54253/AN N13161/DA KDEN/DS KSGF/OT 0035/FB   60/BF
6   DT DDL DEN 010035 M93A
7   ^C
```

from here on i started trying to find journalists interested in a probably pretty broad breach of US aviation. which unfortunately got peoples hopes up in thinking i was behind the TSA problems and groundings a day earlier, but unfortunately im not quite that cool. so while i was waiting for someone to respond to my call for journalists i just kept digging, and oh the things i found.

as i kept looking at more and more config files in more and more of the projects, it dawned on me just how heavily i had already owned them within just half an hour or so. hardcoded credentials there would allow me access to navblue apis for refueling, cancelling and updating flights, swapping out crew members and so on (assuming i was willing to ever interact with a SOAP api in my life which i sure as hell am not).

i however kept looking back at the two projects named `noflycomparison` and `noflycomparisonv2`, which seemingly take the TSA nofly list and check if any of commuteair's crew members have ended up there. there are hardcoded credentials and s3 bucket names, however i just cant find the actual list itself anywhere. probably partially because it seemingly always gets deleted immediately after processing it, most likely specifically because of nosy kittens like me.



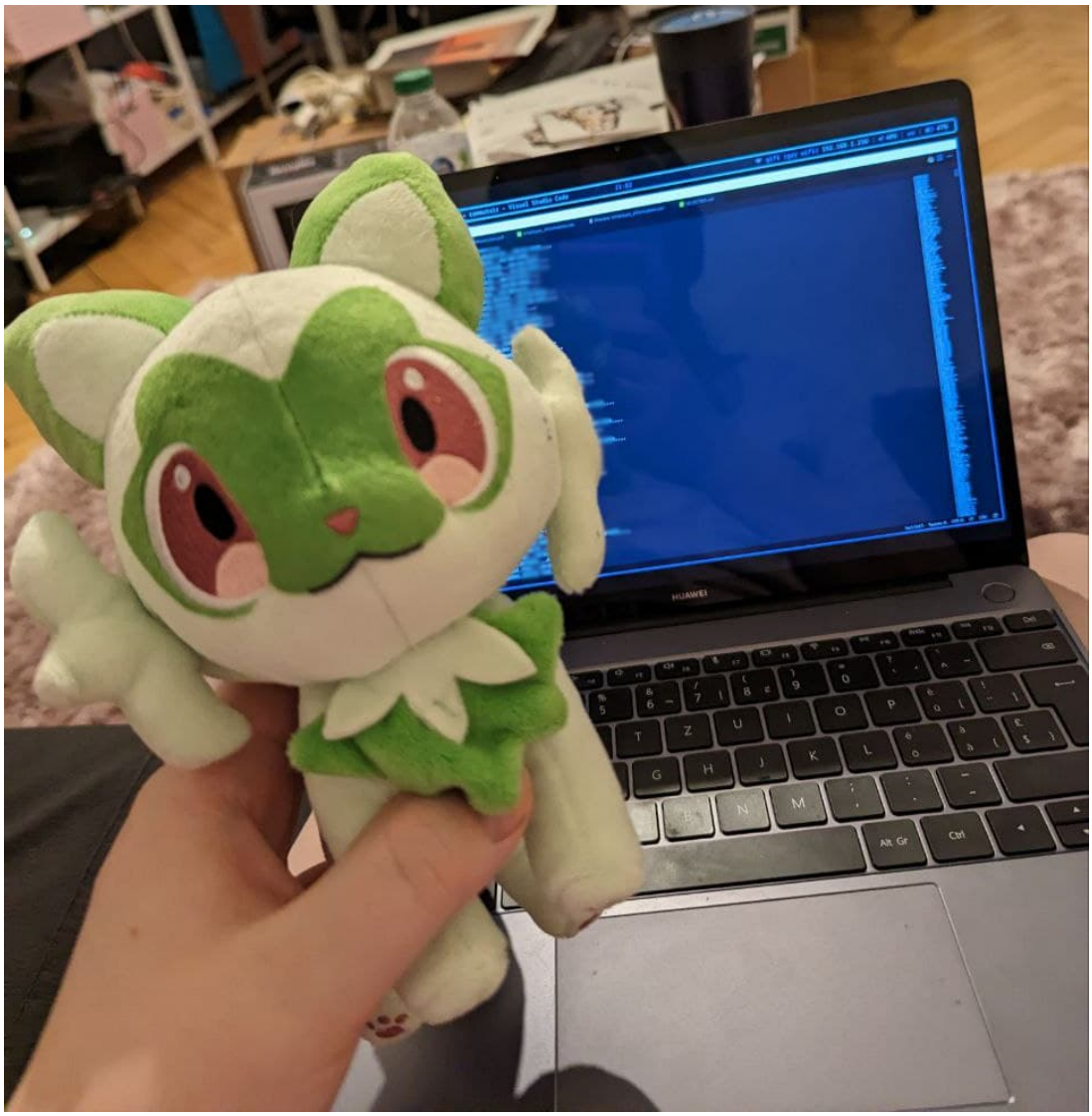
fast forward a few hours and im now talking to Mikael Thalen, a staff writer at dailydot. i give him a quick rundown of what i have found so far and how in the meantime, just half an hour before we started talking, i have ended up finding AWS credentials. i now seemingly have access to pretty much their entire aws infrastructure via `aws-cli`. numerous s3 buckets, dozens of dynamodb tables, as well as various servers and much more. commute really loves aws.

```
~/bounty/commutair  17:34:17
$ aws s3 ls
2022-12-15 02:11:14 aws-cloudtrail-logs-353966347147-2b88e
969
2022-12-15 02:16:46 aws-cloudtrail-logs-353966347147-75a13
43e
2018-07-12 19:46:01 aws-logs-353966347147-us-east-1
2022-12-14 23:36:03 awslogsalb
2020-12-07 18:52:16 c5-integration-builds
2019-10-22 07:56:51 ca-dynamodb-bkp
2017-09-29 17:37:34 ca-ip-dev-s3
2017-11-27 06:44:57 ca-ip-prod-s3
2017-12-01 09:10:35 cf-templates-1l1lipqerp78m-us-east-1
2022-10-29 17:13:14 cf-templates-1l1lipqerp78m-us-east-2
2017-06-30 20:42:09 elasticbeanstalk-us-east-1-35396634714
7
2020-10-23 21:57:45 flightrelease
2020-10-28 20:42:16 fligtrelease-backup
2021-06-09 09:06:40 prod-amos-archive-bucket
2021-09-14 17:19:55 prod-blankgendec-pdf
2021-06-09 09:06:40 prod-company-document-bucket
2021-06-09 09:06:40 prod-crew-archive-bucket
2022-01-14 06:54:44 prod-daily-fa-reads-pdf-store
2021-09-14 17:27:30 prod-daily-pilot-reads-pdf-store
2022-11-10 16:27:00 prod-ecs-container-logs
2021-06-09 09:06:40 prod-flifo-archive-bucket
2021-09-14 16:40:07 prod-fltplan-outbound-eff-store
2021-09-14 16:40:07 prod-fltplan-outbound-pdf-store
2022-05-23 19:02:18 prod-formurl
2021-06-09 09:06:4
2021-06-09 09:06:4
2021-06-09 09:06:4
2021-09-14 17:20:2
2021-09-17 07:32:2
2022-09-13 18:24:3
2022-06-27 20:15:5
2022-09-13 18:24:3
2022-10-17 06:10:2
2022-09-13 18:24:3
2022-11-11 20:54:2
2022-07-27 03:48:1
2021-06-09 09:06:4
2021-06-09 09:06:4
2021-09-23 21:25:4
ore
2021-06-09 09:06:4
2021-05-31 13:52:4

~/bounty/commutair  17:12:46
$ aws dynamodb list-tables
{
    "TableNames": [
        "AlertHistoryTest",
        "AlertHistoryTest1",
        "AlertTest",
        "C5GlobalTest",
        "C5_Activities",
        "C5_AirportCode_TimeZone",
        "C5_CASS_KCM_Requests",
        "C5_CREW_OOS",
        "C5_Calendar_V1",
        "C5_Crew_Vacation",
        "C5_FlightPlanStore",
        "C5_FlightScheduleDiff",
        "C5_Flights",
        "C5_FltPlanRecord"
```

i also share with him how close we seemingly are to actually finding the TSA nofly list, which would obviously immediately make this an even bigger story than if it were "only" a super trivially ownable airline. i had even peeked at the nofly s3 bucket at this point which was seemingly empty. so we took one last look at the noflycomparison repositories to see if there is anything in there, and for the first time actually take a peek at the test data in the repository. and there it is. three csv files, `employee_information.csv`, `NOFLY.CSV` and `SELECTEE.CSV`. all commited to the repository in july 2022. the nofly csv is almost 80mb in size and contains over 1.56 million rows of data. this HAS to be the real deal (we later get confirmation that it is indeed a copy of the nofly list from 2019).

holy shit, we actually have the nofly list. holy fucking bingle. what?! :3



with the jackpot found and being looked into by my journalism friends i decided to dig a little further into aws. grabbing sample documents from various s3 buckets, going through flight plans and dumping some dynamodb tables. at this point i had found pretty much all PII imaginable for each of their crew members. full names, addresses, phone numbers, passport numbers, pilot's license numbers, when their next linecheck is due and much more. i had trip sheets for every flight, the potential to access every flight plan ever, a whole bunch of image attachments to bookings for reimbursement flights containing yet again more PII, airplane maintenance data, you name it.

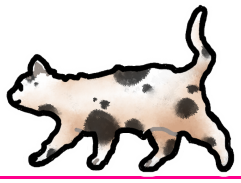
i had owned them completely in less than a day, with pretty much no skill required besides the patience to sift through hundreds of shodan/zoomeye results.

so what happens next with the nofly data

while the nature of this information is sensitive, i believe it is in the public interest for this list to be made available to journalists and human rights organizations. if you are a journalist, researcher, or other party with legitimate interest, the data is available for access (upon request) via DDoSecrets.

support me

if you liked this or any of my other security research feel free to support me on my ko-fi. i am unemployed and in a rather precarious financial situation and do this research for free and for the fun of it, so anything goes a lonɛ way.



---

rss feed | tumblr | fedded verse | sounded cloud | last dot federated states of micronesia | gitted hub | gitted tea | ko-fi | reddit

credits: maia kitten art by vai5000, pixel art maia kitten by A. Marmot and pointer following kitten code from adryd325/oneko.js

This site is part of the lavender.software webring!

← oatmealine maia easrng →

sleepy.zone webring!

← tayxm maia sadgirlsclub →